SEGURIDAD CIBERNÉTICA 101

CONSEJOS PARA MANTENER LA SEGURIDAD DE SUS CUENTAS VIRTUALES

DISTRIBUIDO OCTUBRE 2021

Nellie M. Gorbea
Secretaria de Estado

Estimado votante de Rhode Island,

Octubre es el mes de Sensibilización de la Seguridad Cibernética. Como su Secretaria de Estado, es mi responsabilidad garantizar que usted pueda ejercer su derecho a votar de forma segura y protegida. También soy muy consciente de las estafas más comunes que dejan a los votantes expuestos a los crímenes cibernéticos y al robo de identidad. Las personas de la tercera edad son con más frecuencia el objetivo de los crímenes cibernéticos, ya que suelen tener mejor crédito y mayores bienes.

Le invito a leer este folleto informativo para proteger su correo electrónico y sus cuentas virtuales, y aprender como identificar estafas. También, he incluido información acerca de como puede revisar de forma segura y protegida la información de su registro de votante, para asegurarse de que usted esté listo para votar en cada elección.

Si tiene algunas preguntas o inquietudes, por favor comuníquese conmigo por correo electrónico en SecretaryGorbea@sos.ri.gov o llamándome al 401.222.2357.

CÓMO DETECTAR LAS ESTAFAS CIBERNÉTICAS MÁS COMUNES

Los criminales cibernéticos saben como hacerse pasar por amigos o miembros de su familia, entidades bancarias, organizaciones benéficas o vendedores virtuales aparentando ser legítimos para robar su información y acceder a sus cuentas financieras y personales. A continuación, le presentamos algunas de las estafas más comunes utilizadas en contra de las personas de la tercera edad de Rhode Island para obtener el acceso a sus cuentas financieras. Si usted ha sido víctima de alguna estafa, haga una denuncia de inmediato a sus autoridades locales.

Emergencia de familia: Los criminales cibernéticos utilizan las redes sociales para recopilar información sobre sus seres queridos. Luego, se ponen en contacto con usted para informarle que uno de sus seres queridos necesita ayuda financiera de forma urgente, ya sea por una lesión adquirida “durante un viaje” o por problemas con la autoridad.

Suplantación del gobierno: Los criminales cibernéticos se hacen pasar por trabajadores del gobierno. Es posible que le amenacen con tomar ciertas acciones a menos que usted haga un pago o le exijan a hacer clic en un enlace para obtener información importante sobre ciertos beneficios.

Servicio de asistencia técnica: Los criminales cibernéticos se hacen pasar por representantes de servicio tecnológico y le ofrecen arreglar problemas informáticos inexistentes.

Servicios financieros: Los criminales cibernéticos se dirigen a sus víctimas potenciales utilizando credenciales ilegítimas de servicios legítimos, como los bancos, las compañías de hipotecas y otras compañías de crédito

TÉRMINOS FRECUENTEMENTE UTILIZADOS

Programa malicioso, "Malware": Es un programa virtual diseñado específicamente para interrumpir, dañar y obtener acceso no autorizado a un computador. Normalmente este programa se instala cuando un usuario hace clic en un enlace malicioso o descarga algún archivo adjunto malicioso enviado por correo electrónico.

Correos electrónicos fraudulentos, "Phishing": Es cuando los criminales cibernéticos envían un correo electrónico o crean un sitio web haciéndose pasar por una empresa u organización legítima para obtener información confidencial, como las contraseñas de cuentas financieras. Por lo general, el contenido de estos correos electrónicos crea una sensación de emergencia para que el usuario abra un archivo adjunto o haga clic en algún enlace, dejando su computador vulnerable.

Programa de secuestro informático, "Ransomware": Es una forma de malware que directamente impide al usuario acceder a los archivos de su computador hasta que pague un "rescate".

Suplantación de identidad por texto, "Smishing": Es cuando los criminales cibernéticos, a través de mensajes de texto enviados a los teléfonos celulares, se hacen pasar por alguna empresa u organización legítima para obtener información personal como las contraseñas o los números de tarjetas de crédito.

Programa espía informático, "Spyware": Es una forma de malware que espía la actividad del usuario, incluyendo las impresiones de las contraseñas y las cuentas financieras.

Virus: Es una forma de malware cuyo objetivo es dañar, borrar o modificar la información de un computador.

Suplantación de identidad por teléfono, "Vishing": Es cuando los criminales cibernéticos, a través del teléfono, se hacen pasar por una empresa u organización legítima para poder obtener información confidencial, como los números de su seguro social. Al igual que los correos electrónicos de phishing, el delincuente creará una sensación de urgencia o emergencia que debe resolverse de forma inmediata.

10 CONSEJOS PARA EVITAR Y PREVENIR LAS ESTAFAS CIBERNÉTICAS

1. No se deje llevar por la urgencia que crea el estafador para que usted actúe rápidamente. Los estafadores son expertos en manipular las emociones y crearán esa emergencia para persuadirle a actuar sin pensar.
2. Nunca envíe dinero o información personal a personas o empresas que no conoce.
3. Desconfíe de cualquier persona que solicite tarjetas de regalo como forma de pago.
4. La mayoría de las empresas y las organizaciones no preguntan sobre su información personal por correo electrónico o por mensaje de texto. Antes de hacer clic en algún enlace o responder a una solicitud urgente, busque la información sobre la empresa o agencia gubernamental que le está contactando.
5. Desconfíe de los regalos o premios "gratis". Si algo parece ser demasiado bueno como para ser real, entonces probablemente lo sea.
6. Sea cuidadoso con lo que descargue. Nunca abra un documento adjunto de un correo electrónico de alguien que usted no conoce y sea cauteloso con los archivos adjuntos en los reenvíos de correos electrónicos de amigos.
7. Desconéctese del internet y apague su computador si le aparece alguna ventana emergente inusual o se bloquea la pantalla.
8. Use un programa de antivirus de calidad y asegúrese actualizarlo regularmente.
9. Asegúrese de que sus contraseñas sean lo suficientemente fuertes y diferentes en los distintos sitios web. *(Vea "Cómo crear contraseñas fuertes" en la página 3.)*
10. ¡Tenga cuidado con lo que comparte en sus redes sociales! *(Vea "Las mejores prácticas para las redes sociales" en la página 3.)*

Señales de Alerta

RECONOZCA LAS SEÑALES DE ALERTA DE LOS CORREOS ELECTRÓNICOS FRAUDULENTOS, 'PHISHING EMAILS'

De: microsoftusertechsupport@gmail.com ← Una dirección de correo electrónico incorrecta.

A: janedoe@sudirecciónde correo.com

Fecha: sábado, septiembre, 3:30 AM ← Un correo enviado a una hora extraña.

Asunto: Actividad del usuario sopechosa

Inicio de sesión inusual

Los errores ortográficos y frases inusuales.

Hemos detectado algo inusual para usar una aplicación móvil para iniciar sesión en su computador Windows. Hemos identificado un sospechoso intento de iniciar sesión en su computadora Windows de un lugar desconocido. Al investigarlo, nuestros oficiales de seguridad descubrieron que alguien con una dirección de IP extranjera trató de realizar una conexión prohibida a su red digital lo que puede corromper su clave de licencia de windows.

Información de inicio de sesión:
País/región: Lagos, Nigeria
Dirección IP: 293.09.101.9
Fecha: 09/07/2016 02:16 AM (GMT)

Un sentido de urgencia.

Si no está seguro de que fue usted, pueda que un usuario malicioso esté tratando de acceder a su red digital. Por favor revise su actividad reciente y le ayudaremos a tomar acciones correctivas. Por favor contacte al Centro de Seguridad de Comunicación y déjenos saber inmediatamente 1-800-816-0380 o sustituir puede también visitar el Sitio Web https://www.microsoft.com/ y completar un formulario de queja del consumidor. Cuando llame, por favor proporcione su número de referencia: AZ-1190 para que nuestros técnicos le puedan ayudar mejor.

Nuestro técnico certificado de Microsoft le proporcionará la mejor solución. Usted ha recibido este aviso por correo obligatorio para informarle sobre cambios importantes a su dispositivo de Windows.

Revisar su actividad reciente ← **Los enlaces indicándole que tome una acción.**
(Desplazar el cursor sobre los enlaces, revela que la dirección de un sitio web [URL por sus siglas en inglés] es diferente a la que aparece en el texto.)

Email image courtesy phishing.org.

LAS MEJORES PRÁCTICAS PARA LAS REDES SOCIALES

Los criminales cibernéticos utilizan las redes sociales como herramientas para recopilar información acerca de usted y de sus seres queridos. ¡Aquí le proporcionamos unos consejos para ser más precavido en las redes sociales!

- Revise sus configuraciones de seguridad y reduzca la cantidad de información personal que comparte públicamente.
- Nunca comparta fechas ni información acerca de un viaje antes de o durante el viaje.
- Sólo acepte la solicitud de amistad de personas que conoce o confía.
- Evite las encuestas y los concursos divertidos. Los estafadores usan estos métodos para conocer las respuestas a las preguntas de seguridad más comunes, como su primera mascota, o información sobre su primer carro o donde y cuando asistió a bachillerato.

CÓMO CREAR CONTRASEÑAS FUERTES

Las contraseñas fuertes ayudan mantener seguras sus cuentas virtuales. Aquí le proporcionamos algunos consejos para crear contraseñas fuertes.

- Escoja contraseñas que tengan significado para usted y nadie más. ***No incluya información que es ampliamente conocida, como las fechas de cumpleaños, fechas de aniversarios, o los apellidos de soltera o los segundos nombres.***
- Evite el uso de palabras. Mejor piense en una frase o la letra de una canción y utilice la primera letra de cada palabra como su contraseña. O reemplace algunas letras con números y caracteres especiales. ¡Los generadores de contraseñas pueden ayudar!
- No utilice la misma contraseña para varias cuentas virtuales. Utilice una aplicación administradora de contraseñas para mantener sus contraseñas de forma organizada y segura.

¡ESTÉ LISTO PARA VOTAR!

¡Es importante asegurarse de tener siempre actualizada la información de su registro de votante! Aquí encontrará los pasos para revisar la información de su registro de votante de forma rápida y sencilla por internet.

1. Visite vote.ri.gov.
2. Haga clic en “Ver/actualizar mi registro de votante”.
3. Rellene los campos requeridos y haga clic en “Continuar”.
4. Esto le llevará a su página de Información de Votante donde puede verificar si su dirección y la afiliación de partido político están correctas. Si todo está actualizado, puede cerrar la ventana de su navegador.
5. Para actualizar su dirección o afiliación de partido político, simplemente haga clic en “Editar su registro”. *Necesitará una licencia de conducir de RI válida para poder iniciar la sesión y modificar su registro de votante.* Siga los pasos para actualizar su información de votante.

   De manera alternativa, puede hacer clic en el enlace para descargar y completar un formulario en papel de inscripción de votante.

SEA UN VOTANTE INFORMADO - AYUDE A ACABAR CON LA MANIPULACIÓN INFORMATIVA

La información falsa es compartida en las redes sociales tanto por error (lo que se conoce como **la desinformación**) como a propósito (lo que se conoce como la **manipulación informativa**). Desafortunadamente, TODA la información falsa publicada en las redes sociales causa confusión en los votantes y esto puede resultar en que desconfíen de la integridad de las elecciones. Usted puede ayudar a acabar con la propagación de información falsa haciéndose las siguientes preguntas:

- ¿Hay varios medios de comunicación reportando la misma noticia o es un sitio de medios menos conocido?
- ¿El título o la imagen de la noticia es escandalosa para atraer clics? ¿Cuál es la historia completa?
- ¿Es el autor creíble? ¿Tiene un amplio historial de reportaje sobre el tema? ¿Se le conoce por escribir noticias, sátira, o artículos de opinión?
- ¿Hay recursos que sustenten la historia?
- ¿Están sus propias creencias afectando su juicio?

Si tiene alguna pregunta, comuníquese con sus funcionarios electorales estatales y locales para hacerles consultas sobre las elecciones en Rhode Island.

Departamento de Estado de Rhode Island | División de Elecciones

148 West River Street, Providence, 02904
401.222.2340 | elections@sos.ri.gov